

**AMENDMENTS TO THE CLAIMS**

Please **AMEND** claims 1, 3, and 6-9 as shown below.

This list of claims will replace all prior versions and lists of claims in the application.

1. (Currently Amended) A method for automatically entering into a secure communication mode in a wireless communication terminal, comprising the steps of:
  - a) storing a voice signal outputted from a vocoder of the wireless communication terminal signal for a predetermined time;
  - b) selecting at least one of the voice signal values among which the occurrence of generation is lower than a threshold value[[,]] to generate a token header data;
  - c) combining token header data of variable lengths to form a token header and generating a token including the token header, the token header data having the lowest occurrence of generation among voice data outputted from [[a]] the vocoder of the wireless communication terminal;
  - d) at a transmission terminal, receiving a request for a secure communication from a user and transmitting the token to a reception terminal; and
  - e) at the transmission terminal, entering into a secure communication mode based on an acknowledge token ~~transmitted~~ received from the reception terminal, and performing secure communication with the reception terminal.
2. (Previously Presented) The method as recited in claim 1, wherein the token includes a data having the lowest generation occurrence among the data of voice packet data outputted from the vocoder as a token header.
3. (Currently Amended) The method as recited in claim 1, wherein the token is shorter

than the maximum length of the voice data outputted from the vocoder.

4. (Original) The method as recited in claim 3, wherein the token includes a key used in an encryption algorithm for the secure communication.

5. (Previously Presented) The method as recited in claim 1, wherein in the step d), the token is transmitted repeatedly a predetermined number of times.

6. (Currently Amended) The method as recited in claim 5, wherein in the step d), the repeated transmission of the token stops when the acknowledge token ~~transmitted~~ from the reception terminal is received.

7. (Currently Amended) The method as recited in claim 1, further comprising the steps of:

f) at the reception terminal, ~~checking-out if~~ receiving the token transmitted from the transmission terminal ~~is received~~, and transmitting ~~[[the]]~~ a token formed in accordance with the step c) ~~[[a]]~~ as ~~[[an]]~~ the acknowledge token to the transmission terminal; and

g) at the reception terminal, entering into ~~[[a]]~~ the secure communication mode and performing secure communication with the transmission terminal.

8. (Currently Amended) The method as recited in claim 7, wherein the step f) includes the step of:

h) ~~checking-out if~~ comparing a session key generated in the transmission terminal and included in the token ~~is matched~~ with a session key generated in the reception terminal using a master key.

9. (Currently Amended) A computer-readable recording medium for recording a program that implements a method for automatically entering into a secure communication mode in a wireless communication terminal provided with a processor, comprising the steps of:

a) combining token header data of variable lengths to form a token header and generating a token including the token header, the token header data having the lowest occurrence of generation among voice data outputted from a vocoder of the wireless communication terminal;

b) at a transmission terminal, receiving a request for a secure communication from a user and transmitting the token to a reception terminal; and

c) at the transmission terminal, entering into a secure communication mode based on an acknowledge token ~~transmitted~~ received from the reception terminal, and performing secure communication with the reception terminal.

10. (Previously Presented) The method of claim 1, further comprising:

combining the token header data to form the token header of a predetermined length.